Department of Defense
INSTRUCTION

SUBJECT: Information Assurance (IA) in the Defense Acquisition System

References: (a) Chapter 25 of title 40, United States Code
              (b) DoD Directive 8500.1, "Information Assurance," October 24, 2002
              (c) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
              (d) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003
              (e) through (k), see enclosure 1

1. PURPOSE

This Instruction:

1.1. Implements policy, assigns responsibilities, and prescribes procedures under references (a), (b), and (c) necessary to integrate information assurance (IA) into the Defense Acquisition System described in reference (d) and DoD Instruction 5000.2 (reference (e)).

1.2. Describes required and recommended levels of IA activities relative to the acquisition of systems and services.

1.3. Describes the essential elements of an Acquisition IA Strategy, its applicability, and prescribes an Acquisition IA Strategy submission and review process.

2. APPLICABILITY AND SCOPE

This Instruction:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. Applies to all acquisitions of automated information systems (AIS), outsourced information technology (IT)-based processes, and platforms or weapon systems with IT interconnections to the Global Information Grid (GIG).

3. DEFINITIONS

Terms used in this Instruction are defined in references (b), (c) and (d), or in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. IA shall be implemented in all system and services acquisitions at levels appropriate to the system characteristics and requirements throughout the entire life cycle of the acquisition.

4.2. All acquisitions of mission critical or mission essential IT systems, as defined in reference (e), shall have an adequate and appropriate Acquisition IA Strategy that shall be reviewed prior to all acquisition milestone decisions, program decision reviews, and acquisition contract awards.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (DoD CIO) shall:

5.1.1. Oversee implementation of this Instruction in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)).

5.1.2. Support the USD(AT&L) in developing guidance necessary to integrate IA into the Defense Acquisition System and the essential elements of an Acquisition IA Strategy submission and review process.

5.1.3. Support the Overarching Integrated Product Teams (OIPT) by ensuring that IA is included for consideration prior to all acquisition milestone decisions, program decision reviews, and acquisition contract awards.

5.1.4. Establish and implement procedures for the review of Acquisition IA Strategies from programs acquiring mission critical or mission essential IT.

5.2. The <u>Under Secretary of Defense for Acquisition, Technology, and Logistics</u> shall:

5.2.1. Ensure that IA is included for OIPT consideration prior to all acquisition milestone decisions, program decision reviews, and acquisition contract awards.

5.2.2. Support the ASD(NII) in overseeing implementation of this Instruction.

5.2.3. Ensure that detailed procedures and processes for implementing IA in defense acquisitions and for developing an Acquisition IA Strategy are incorporated in guidance issued to the defense acquisition workforce.

5.2.4. Ensure that principles and processes for implementing IA in defense acquisitions are included in the education and training of the defense acquisition workforce.

5.3. The <u>Chairman of the Joint of Chiefs of Staff</u> shall:

5.3.1. Provide advice and assessment on military capability needs in accordance with sections 153, 163, and 181 of title 10 U.S.C. (reference (f)). The Chairman shall present this advice and assessment through validated and approved Joint Capabilities Integration and Development System documents (see Chairman of the Joint Chiefs of Staff Instructions 3170.01 and 6212 Series (reference (g) and (h))). The Chairman may engage the DoD Components and Agencies to provide this advice and assessment.

5.3.2. Consistent with this Directive, in coordination with the USD(AT&L) and the ASD(NII), the Chairman may establish procedures to carry out this responsibility.

5.4. The <u>Director, National Security Agency</u> shall provide support and guidance, as required, to Program Managers in developing an IA approach, and obtaining information systems security engineering services, to include describing information protection needs, defining and designing system security to meet those needs, and assessing the effectiveness of system security.

5.5. The <u>Heads of the DoD Components</u> shall:

5.5.1. Ensure that IA is implemented in all system and service acquisitions in accordance with USD(AT&L) guidance, as issued.

5.5.2. Establish and implement internal management processes for the preparation and review of Acquisition IA Strategies at the DoD Component levels.

5.5.3. Designate a principal point of contact to represent the Component on policy and procedural matters regarding IA in the acquisition system.

5.5.4. Establish and implement procedures for the submission and review of Acquisition IA Strategies from programs acquiring IT other than mission critical or mission essential IT, as desired.

5.6. The <u>Program Managers</u> shall ensure that IA is fully integrated into all phases of their acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, and operation.

6. <u>PROCEDURES</u>

6.1. Program Managers and other acquisition officials shall comply with the policy and procedures of references (b) and (c) for all acquisitions, except where the system or service being acquired does not utilize any IT, or where the IT component of the system being acquired consists solely of platform IT with no interconnection to external information systems or networks.

6.2. Significant features of compliance include:

6.2.1. Appointment of an IA Manager.

6.2.2. Determination of system Mission Assurance Category (MAC) and Confidentiality Level.

6.2.3. Identification and implementation of appropriate system Baseline IA Controls according to enclosure 4 of reference (c).

6.2.4. Planning and execution of the certification and accreditation process according to DoD Instruction 5200.40 (reference (i)) and DCI Directive 6/3 (reference (j)), if applicable.

6.3. Program Managers shall also provide updated program IA status to OIPTs and Integrating Integrated Product Teams.

6.4. Acquisition IA Strategy

6.4.1. Submission Requirements. Program Managers for acquisitions that include IT and are designated "Mission Critical" or "Mission Essential" systems as defined in reference (e), shall prepare and submit an Acquisition IA Strategy addressing the topics specified in USD(AT&L) IA guidance, as issued. The Heads of the DoD Components may develop submission requirements for Acquisition IA Strategies for all other acquisitions as they deem appropriate.

6.4.2. Review Process. Acquisition IA Strategies for all Acquisition Category (ACAT) IAM, ACAT IAC, and ACAT ID programs shall be approved by the DoD Component CIO and submitted to the DoD CIO for review prior to all acquisition milestone decisions, program decision reviews, and acquisition contract awards. The Heads of the DoD Components are delegated the authority to conduct reviews of Acquisition IA Strategies on the behalf of the DoD CIO for all other acquisitions, and may delegate authority to approve Acquisition IA Strategies. The results of all reviews shall be documented and retained.

7. EFFECTIVE DATE

This Instruction is effective immediately.

Linton Wells II
Acting Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Enclosures - 2
E1. References, continued
E2. Definitions

E1. <u>ENCLOSURE 1</u>

<u>REFERENCES</u>, continued

(e) <u>DoD Instruction 5000.2</u>, "Operation of the Defense Acquisition System,"
     May 12, 2003
(f) Sections 153, 163, and 181 of title 10, United States Code, "Armed Forces"
(g) CJCSI 3170.01, Series, "Joint Capabilities Integration and Development System,"
     current edition
(h) CJCSI 6212.01, Series, "Interoperability and Supportability of Information
     Technology and National Security Systems," current edition
(i) <u>DoD Instruction 5200.40</u>, "DoD Information Technology Security Certification and
     Accreditation Process (DITSCAP)," December 30, 1997
(j) DCI Directive 6/3, "Protecting Sensitive Compartmented Information Within
     Information Systems," June 5, 1999
(k) OMB Circular A-130, "Management of Federal Information Resources,
     Transmittal 4," November 30, 2000

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. <u>Acquisition Program</u>. A directed, funded effort that provides new, improved, or continuing materiel, weapon, or information system or service capability in response to an approved need.

E2.1.2. <u>Automated Information System (AIS)</u>. See DoD Information System.

E2.1.3. <u>Confidentiality Level</u>. Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has defined three confidentiality levels: classified, sensitive, and public.

E2.1.4. <u>Data</u>. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned.

E2.1.5. <u>DoD Information System</u>. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

E2.1.5.1. <u>Automated Information System (AIS) Application</u>. For DoD IA purposes, an AIS application is the product or deliverable of an acquisition program such as those described in reference (d). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note: An AIS application is analogous to a "major application" as defined in OMB A-130 (reference (k)); however, this term is not used in

order to avoid confusion with the DoD acquisition category of Major Automated Information System (MAIS).

E2.1.5.2. Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest Mission Assurance Category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves are analogous to general support systems, as defined in reference (k). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

E2.1.5.3. Outsourced IT-based Process. For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

E2.1.5.4. Platform IT Interconnection. For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems, such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

E2.1.6. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD process for identifying information security requirements, providing security solutions, and managing information system security activities.

E2.1.7. <u>Enclave</u>. See DoD Information System.

E2.1.8. <u>Global Information Grid (GIG)</u>. Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in reference (a). The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or shall not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.8.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

E2.1.8.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.8.3. Processes data or information for use by other equipment, software, and services.

E2.1.9. <u>IA Control</u>. An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with reference (k).

E2.1.10. <u>Information</u>. Any communication or representation of knowledge, such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

E2.1.11. <u>Information Assurance (IA)</u>. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.12. <u>Information Technology (IT)</u>. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that requires the following:

E2.1.12.1. The use of such equipment; or

E2.1.12.2. The use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

E2.1.13. <u>Major Automated Information System (MAIS)</u>. An acquisition program where the dollar value estimated by the DoD Component Head is to require program costs (all appropriations) in any single year in excess of $32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of $126 million in FY 2000 constant dollars, or total life-cycle costs in excess of $378 million in FY 2000 constant dollars, or Milestone Decision Authority designation as special interest.

E2.1.14. <u>Mission Assurance Category (MAC)</u>. Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

E2.1.14.1. <u>Mission Assurance Category I (MAC I)</u>. Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and

timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

E2.1.14.2. <u>Mission Assurance Category II (MAC II)</u>. Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

E2.1.14.3. <u>Mission Assurance Category III (MAC III)</u>. Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

E2.1.15. <u>Mission Critical Information System</u>. A system that meets the definitions of "information system" and "national security system" in reference (a), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the USD(Comptroller). A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System.")

E2.1.16. <u>Mission Essential Information System</u>. A system that meets the definition of "information system" in reference (a), that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the USD(Comptroller). A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System.")

E2.1.17. <u>Outsourced IT-based Process</u>. See DoD Information System.

E2.1.18. <u>Platform IT Interconnection</u>.   See DoD Information System.

E2.1.19. <u>Program Manager (PM)</u>.   The designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs.   The PM shall be accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority.

E2.1.20. <u>Weapon(s) System</u>.   A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.